DOCUMENT RESUME

ED 476 087 SE 067 788

AUTHOR Rowland, Tim

TITLE Proofs in Number Theory: History and Heresy.

PUB DATE 2002-07-00

NOTE 7p.; In: Proceedings of the Annual Meeting of the International Group for the Psychology of Mathematics Education (26th, Norwich, England, July 21-26, 2002; see SE 067 806.

PUB TYPE Opinion Papers (120) -- Speeches/Meeting Papers (150)

EDRS PRICE EDRS Price MF01/PC01 Plus Postage.

DESCRIPTORS Elementary Secondary Education; *Mathematics Instruction; Teaching Methods; Thinking Skills

ABSTRACT

The domain of number theory lends itself particularly well to generic argument, presented with the intention of conveying the force and structure of a conventional generalized argument through the medium of a particular case. The potential of generic examples as a didactic tool is virtually unrecognized. Although the use of such examples has good historical provenance, the suggestion that they might be an alternative to formal proof tends to be viewed as a kind of heresy from the perspective of modern proof practice. This paper discusses the advantages of using particular-but-generic proof strategies in undergraduate classrooms and in textbooks in order to convince students of the truth of number-theoretic theorems and student-generated conjectures. (KHR)

Reproductions supplied by EDRS are the best that can be made from the original document.

ED 476 087

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY

J. Van Dormolen

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

1

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

PROOFS IN NUMBER THEORY: HISTORY AND HERESY

Tim Rowland
University of Cambridge

My purpose in writing this paper is to advocate the use of particular-but-generic proof strategies in undergraduate classrooms and in textbooks, in order to convince students of the truth of number-theoretic theorems and student-generated conjectures. The domain of number theory lends itself particularly well to generic argument, presented with the intention of conveying the force and the structure of a conventional generalised argument through the medium of a particular case. The potential of the generic example as a didactic tool is virtually unrecognised. Although the use of such examples has good historical provenance, the suggestion that they might be an alternative to formal proof tends to be viewed as a kind of heresy from the perspective of modern proof practice.

Procedures and proofs

The use of examples to point to abstract concepts and to general *procedures* is commonplace pedagogical practice (see e.g. Mason's paper for this research forum). In the field of number theory, a case in point might be explication of the Euclidean algorithm for the greatest common divisor of two natural numbers. Beginning with, say, 194 and 40 the demonstration proceeds:

$$\begin{aligned} 194 &= 4 \times 40 + 34 \\ 40 &= 1 \times 34 + 6 \\ 34 &= 5 \times 6 + 4 \\ 6 &= 1 \times 4 + 2 \\ 4 &= 2 \times 2 + 0 \end{aligned}$$

In order to apply the procedure to another pair of natural numbers, the student needs to become aware of the status of each number in each row of the procedure, and how each row relates to the next. That is, not only to agree that each line is a true statement, but to appreciate how it has been initiated and structured. As teacher, I might assist this by (say) underlining the quotients 4, 1, 5, 1, 2 in red. I might draw diagonal lines joining the divisor and remainder in each line to the dividend and divisor, respectively, in the next e.g. joining the two 40s, the two 34s, and so on. (It is relevant to pause to reflect on how you made sense of the previous sentence: perhaps the example was more illuminating than the somewhat archaic expression of the general procedure that preceded it.) The choice of example (194, 40) was made in recognition of its merits in its own right and relative to some alternatives. I judge it to be preferable to (194, 48), which is a poor paradigm because, for that pair, the algorithm terminates too soon. I would also avoid (144, 89) for a different reason: although it has good 'length', it conveys difference rather than division. Try it, if the intention of that remark is not self-evident. I would resist (97, 20) in recognition of my own liking for coprime pairs despite their particularity.

Much less common is the use of examples to explain why general relationships might hold: in short, to *prove*. One reason why this might be the case is clear enough—because

BEST COPY AVAILABLE

ED 476 087

one or more examples cannot prove a statement about an infinite category of cases. Yet there is a sense in which the *presentation* of a single example can speak for some general truth, and for some general argument above and beyond the particularities of the example itself. Such examples, suitably structured to be not just a confirming instance but a chain of reasoning, are known as generic examples. As Balacheff (1988) so clearly and elegantly puts it:

> The generic example involves making explicit the reasons for the truth of an assertion by means of operations or transformations on an object that is not there in its own right, but as a characteristic representative of the class. (Balacheff, 1988, p. 219)

The generic example serves not only to present a confirming instance of a proposition - which it certainly is - but to provide insight as to *why* the proposition holds true for that single instance. The transparent presentation of the example is such that analogy with other instances is readily achieved, and their truth is thereby made manifest. Ultimately the audience can conceive of no possible instance in which the analogy could not be achieved.

Un peu d'histoire

The story (probably apocryphal, but see Polya, 1962, pp. 60-62 for one version) is told about the child C. F. Gauss, who astounded his village schoolmaster by his rapid calculation of the sum of the integers from 1 to 100. Whilst the other pupils performed laborious column addition, Gauss added 1 to 100, 2 to 99, 3 to 98, and so on, and finally computed fifty 101s with ease. The power of the story is that it offers the listener a means to add, say, the integers from 1 to 200. Gauss's method demonstrates, by generic example, that the sum of the first $2k$ positive integers is $k(2k+1)$. Nobody who could follow Gauss' method in the case k=50 could possibly doubt the general case. It is important to emphasise that it is not simply the *fact* that the proposition $1+2+3+ \ldots + 2k = k(2k+1)$ has been verified as true in the case k=50. It is the *manner* in which it is verified, the form of presentation of the confirmation.

Paul Hoffman recounts the story in his best-seller *The Man Who Loved Only Numbers* (Hoffman, 1998). His comment on it (quoting mathematician Ronald Graham) is a telling testimony to the genericity of Gauss' method.

> What makes Gauss' method so special .... Is that it doesn't just work for this specific problem but can be generalised to find the sum of the first 50 integers or the first 1,000 integers ... or whatever you want. (p. 208)

In introducing the notion 'generic example' to audiences of all kinds - undergraduate and graduate students, mathematics education conference-goers, 'general audiences' - I routinely choose Gauss' method as a paradigm of the genre. We should not be surprised that Gauss, of all people, should have provided it. Ironically, his *Disquisitiones Arithmeticae* established the 'modern' standard for generality in number theoretic proof arguments.

BEST COPY AVAILABLE

By contrast, Pierre de Fermat (1601-65) was notorious for stating number theoretic results in the absence of formal proof. In particular, it was Euler who gave a general proof of the 'Little' Theorem (if p is prime and a, an integer, p divides a^p-a) some decades after Fermat stated it. In a recent article, Burn (2002) offers some suggestions concerning the kinds of reasoning that Fermat himself might have used to establish the truth of some claims associated with his Little Theorem, made in a letter to Mersenne in 1640. These claims were developed in the course of Fermat's search for perfect numbers. A natural number (such as 6 or 28) is said to be *perfect* if it is equal to the sum of its divisors including 1, but not itself. Around 300BC, Euclid had established that the set of perfect numbers can be identified with integers of the form $2^{n-1}(2^n - 1)$ where $2^n - 1$ is prime. In his letter to Mersenne (after whom such primes are named), Fermat claimed that if n is composite then $2^n - 1$ is not prime. The proof amounts to the observation that $2^a - 1$ divides $2^{ab} - 1$. The converse, however, is false: in 1536, Hudalrichus Regius had shown that although 11 is prime, $2^{11} - 1$ is composite, and so $2^{10}(2^{11} - 1)$ is not a perfect number.

Fermat made a claim which was to transform the previously Herculean task of determining whether or not $2^p - 1$ is prime for a given prime p. In effect, Fermat claimed that if an integer of this form has a prime factor, then that factor is of the form $2kp + 1$ (the factor 1 is covered by k=0, and it follows from Fermat's Little Theorem that $2^p - 1$ itself is of the form $2kp + 1$). Thus, to decide whether a proper factor of $2^{11} - 1$ exists, we only need to consider 23, since this is the *only* prime of the form $22k + 1$ with square less than $2^{11} - 1$. In fact, $2^{11} - 1 = 23 \times 89$. (Note that 89 is also of the form $22k + 1$, as expected).

In his letter, Fermat exemplifies this statement about prime factors of $2^p - 1$ with reference to this case i.e. when $p = 11$. Burn (*ibid.*) reconstructs the argument that Fermat might have given with reference to this particular-but-generic case. Burn then continues: "Now we generalise the generic example of factorising $2^{11} - 1$ by expressing the argument algebraically". Of course, this accords with good modern practice, although Burn does not suggest that Fermat, having established the generic, then required the general formulation to be convinced of the general case.

Teaching and learning Wilson's theorem

The obscure Cambridge mathematician John Wilson is remembered to this day on account of a theorem stated in 1770, a century after Fermat's demise:

p is prime if and only if $(p-1)! = -1 \pmod{p}$

To be precise, it was Edward Waring, Isaac Newton's successor (and Stephen Hawking's predecessor) as the Cambridge Lucasian Professor of Mathematics, who stated the result of his former student, Wilson. In the best traditions of the time, neither Wilson nor Waring managed to prove the theorem: its status seems to have been a conjecture, the outcome of inductive reasoning from examples. It fell to Lagrange to give the first proof of Wilson's theorem, in 1773. How then, might we approach the genesis of the theorem and the construction of its proof with the hindsight and didactic insights of the twenty-first century? What might a generic proof of that theorem look like?

BEST COPY AVAILABLE

As a preliminary, we would need to know that ±1 are the only self-inverse elements under multiplication modulo p. Now consider the prime number 13 (17 or 19 would do equally well) and list the reduced set of residues modulo 13:

1 2 3 4 5 6 7 8 9 10 11 12

Pair each of the numbers from 2 to 11 with its (distinct) multiplicative inverse mod 13: (2, 7), (3, 9), (4, 10), (5, 8), (6, 11). 1 and 12, of course, are self-inverse. [I usually link the elements in the inverse-pairs with lines on a chalk board]. Clearly, the product of these integers from 2 to 11 must be congruent to 1^5, i.e. 1, modulo 13. Therefore $12! \equiv 1x1x12$ (=12) mod 13. The argument is generic, since 13 was in no way an untypical choice: the pairing would work equally well with any prime.

The scene now shifts to a session with class of about 20 first-year undergraduate joint honours mathematics-with-education students. I could have stated Wilson's theorem and proved it formally in five minutes. In fact, it took an hour to make some conjectures and to work on proof. This is what happened.

First, I asked them to evaluate 4! mod 5, 6! mod 7, 10! mod 11, and to write down a conjecture. The most common version of the conjecture was $n! \equiv n \bmod (n+1)$. The 'for all n' seemed to be implicit. I asked them to evaluate 5! mod 6. They did, and they were visibly surprised by the refutation. I asked whether they could modify the conjecture. At first they homed in on the even/odd distinction between moduli, but n=8 led to further refutation and eventual restriction to prime values of n+1. n=12 provided a further confirming instance. I proceeded to an interactive presentation of a generic proof, inviting Sonia to pick a prime between 11 and 19. She chose 19. I got them to list 1 to 18 and work on inverse pairs in table-groups, during which Simon spontaneously explained to his colleagues why 18! *had* to be 18 mod 19. I asked him to repeat his reasoning to the class, and wrote his explanation on the whiteboard. He picked out eight inverse pairs, and explained why the product of the integers from 2 to 17 inclusive would have to be 1 mod 19. They dutifully copied Simon's argument. Later, I enquired what would have happened if we had looked at 28! mod 29, and Abby explained why it would have to be 28, again referring to inverse pairings of the integers from 2 to 27, although without feeling the need to identify the pairs this time. "Does everyone agree?", I asked. They agreed. One shouldn't read too much into such consent, however pleasing; nevertheless, Abby, at least, had convinced me that she had appropriated the proof-scheme.

The next day, at a tutorial meeting, I asked five members of the class to write it out the proof (that, for primes p, $p! \equiv p-1 \bmod p$) in conventional generality. Their responses were unaided and individual. It should be borne in mind, as I indicated earlier in this paper, that these students will have had little experience of composing formal proofs. Nevertheless, they all indicated in their writing that the genericity of the case p=19 had been apparent to them. Moreover, their argumentation and use of notation would have satisfied any examiner. Hannah's response, which was typical, was as follows.

$(p-1)(p-2)(p-3)(p-4) \ldots 2x1$

BEST COPY AVAILABLE

Every element of M_p[1] has an inverse, because M_p is a group.

We know (from work on primitive roots) that only p-1 has order 2. Therefore p-1 is self-inverse. All other members of M_p apart from 1 must have a distinct inverse.

Each inverse pair when multiplied gives 1 mod p.

This gives $(p\text{-}1)(1^{1/2(p-3)})1 \equiv (p\text{-}1)!$ mod p

Therefore $(p\text{-}1)! \equiv (p\text{-}1)$ mod p

Only Zoë gave evidence of some insecurity in this intangible world that lies beyond examples. Her proof was much the same as Hannah's, but began with identification of the inverse pairs in the case p=11 (transfer to other examples) and concluded the comment:

> I tried to find a formula for the inverses, for example p-2 has inverse p-6 (but only for p=11). I have been unable to do this.

For Zoë, mere knowledge of the *existence* of distinct inverses in the range 2 to p-2 is not enough. What is not clear is whether it leaves *her* cognitively insecure, or whether she believes that I (in my role as assessor) will expect more.

Abby's proof was elegantly and lucidly expressed, but stated that there are $^1/_2(p\text{-}1)$ inverse-pairs rather than $^1/_2(p\text{-}3)$. A case an error of manipulation, but not one of conception.

Generic arguments and cognitive unity

The domain of elementary number theory lends itself remarkably well to generic argument, presented with the intention of conveying the force and the structure of a conventional generalised argument through the medium of a particular case. One reason for this might be that, in the choice of examples, one seems to be spoiled for choice: there are an awful lot of integers (or primes, or whatever subset is called for) compared, say, with groups, or topological spaces. This is not to say that the choice of a generic example is an arbitrary one: it can be (and in a sense, it *ought* to be) a conscious pedagogical act. Some examples work better than others do for particular purposes - they carry and convey the generalisation rather better because the salient operations on the variable(s) can easily be tracked through the argument. Some tentative principles for the selection of generic arguments and the construction of generic arguments in number theory are given in Rowland (2002). I conclude, however, with some cautionary remarks.

First, the proof of Wilson's theorem given above crucially depends on knowing and being certain that 1 and p-1 are the only self-inverse elements under multiplication mod p. How shall we establish that result? It emerges readily (as a conjecture, of course) from examples, especially when the contrast is made with non-prime moduli. The usual proof runs as follows: if $1 \le a \le p\text{-}1$, and $a^2 \equiv 1$ mod p, then $p \mid (a\text{-}1)(a+1)$ and so $p \mid (a\text{-}1)$ or $p \mid (a+1)$. Whence a=1 or a=p-1. The essence of this argument is the solution of a

[1] M_p denotes the group {1, 2, 3, ..., p-1} under multiplication mod p.

BEST COPY AVAILABLE

quadratic equation in a multiplicative modular group, which seems to rule out a generic presentation entirely free of algebraic symbolism. It is true that I could take p to be 13, and argue that a must be 1 or 12, but I can't seem to side-step arguing from (and with) $13 \mid (a-1)(a+1)$. Perhaps someone will delight me by convincing me that I'm wrong on this point.

Secondly, the converse of Wilson's theorem [if n is composite then $(n-1)! \neq n-1 \bmod n$] *appears* to lend itself wonderfully well to generic exposition. Take the case n=10. Now 9!=362880, so $9! \equiv 0 \bmod 10$. Yes, but why? Because 9! includes factors 2 and 5. Since 10 is composite it can be decomposed into the product of two factors, both strictly between 1 and 10, so both occur as terms in 9! It is thus apparent that if n is composite then:
$(n-1)! \equiv 0 \bmod n$

However, whilst this conclusion is certainly true, the argument does not, in fact, transfer to all composite numbers. In those special cases when n is the square of a prime p, the only possible decomposition of n into the product of two factors, both strictly between 1 and p-1, is $n = p \times p$. The factors are not distinct and it is not the case that both occur as terms in $(n-1)!$ It is not difficult to make a separate argument for these cases, but they can easily be overlooked, and caught in the shadow, as it were, of the earlier generic argument.

Notwithstanding these cautionary words, there seems to be a good prospect of developing and offering a systematic didactic technology of formal proof in number theory, building on skilfully-constructed generic examples. There is evidence that such an approach to proof is supportive of the *cognitive unity* of theorems, that is to say "the continuity ... between the process of statement production and the process of its proof, as well as providing meaningful examples". (Mariotti, Bartolini Bussi, Boero, Ferri and Garuti, 1997).

References

Balacheff, N. (1988). 'Aspects of proof in pupils' practice of school mathematics' in Pimm, D.(Ed) *Mathematics, Teachers and Children.* London, Hodder and Stoughton, (pp. 216-235).

Burn, R. P. (2002, in press). 'Fermat's little theorem – proofs that Fermat might have used.' *Mathematical Gazette* Volume 86 Number 506.

Hoffman, P. (1998). *The Man Who Loved Only Numbers.* London, Fourth Estate.

Mariotti, M. A.; Bartolini Bussi, M.; Boero, P.; Ferri, F.; Garuti, R. (1997). 'Approaching geometry theorems in contexts' in E. Pehkonen (Ed.) *Proceedings of the 21st Conference of the International Group for the Psychology of Mathematics Education* Volume 1, (pp. 180-195). Lahti, Finland: University of Helsinki.

Polya, G. (1962). *Mathematical Discovery, Volume I.* New York, John Wiley.

Rowland, T. (2002). 'Generic proofs in number theory.' In S. Campbell and R. Zazkis (Eds.) *Learning and teaching number theory: Research in cognition and instruction.* (pp. 157-184). Westport, CT: Ablex Publishing.

BEST COPY AVAILABLE

U.S. Department of Education
Office of Educational Research and Improvement (OERI)
National Library of Education (NLE)
Educational Resources Information Center (ERIC)

NOTICE

Reproduction Basis

X	This document is covered by a signed "Reproduction Release (Blanket)" form (on file within the ERIC system), encompassing all or classes of documents from its source organization and, therefore, does not require a "Specific Document" Release form.
	This document is Federally-funded, or carries its own permission to reproduce, or is otherwise in the public domain and, therefore, may be reproduced by ERIC without a signed Reproduction Release form (either "Specific Document" or "Blanket").